Forensic Analysis of Frozen Hard Drive Using Static Forensics Method

By Imam Riadi

International Journal of Computer Science and Information Security (IJCSIS),
Vol. 15, No. 1, January 2017

Forensic Analysis of Frozen Hard Drive Using Static Forensics Method

Faiz Albanna
Department of Informatics
Islamic University of Indonesia
Yogyakarta, Indonesia
faiz.albanna@gmail.com

Imam Riadi
Department of Information Systems
Ahmad Dahlan University
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

***Abstract*— Storage on a computer is volatile (RAM) and non-volatile (Hard Drive). This research concerned about the hard drive storage of non-volatile with the FAT32 file system that uses the Microsoft Windows Operating System pre-installed Deepfreeze software. All activities to be written on the hard drive partitions which were frozen by Deepfreeze software (frozen hard drive) will be returned when the computer restarting or shutdown. That could be difficult to find digital evidence in a crime if frozen hard drive has been installed on the computer (evidence) because the digital evidence will be lost when the computer is off. Static forensics methods are used when obtaining evidence (computer) is off, the acquisition and analysis can be done perform without turning on the computer. The process to find digital evidence related to file recovery, which is a method to restore data or recover deleted file because there is no longer listed in the file system. In this research, the methods method to find the digital evidence were using file recovery, a technique of carving by type, search by a text string and search by hex value. Digital evidence discovered in the form of image files, document files, Internet history logs, and open recent log, which is located in the unallocated space.**

Keywords: Digital Forensics; Hard Drive Forensics; Static Forensics; Frozen Hard Drive; File Recovery

I. INTRODUCTION

Computer forensics can be used as a tool for perpetrators of computer crime such as theft, embezzlement, and others. Evidence from the computer has appeared in court almost 30 years. A simple definition of computer forensics is a set of procedures for conducting thorough testing on a computer system by using software and tools to restore and preserve evidence in a criminal action (1).

In Indonesia, the case of computer crime is increasing every year. In the last decade, there were 563 cases of computer crime with the total number of items of electronic evidence as much as 3,130 units. These statistics show that computer crime is a serious problem in the digital era. Full case of computer crime and computer related crime addressed by Digital Forensic Laboratory of Police Headquarters in 2006 to 2015 is shown in figure 1 (2).

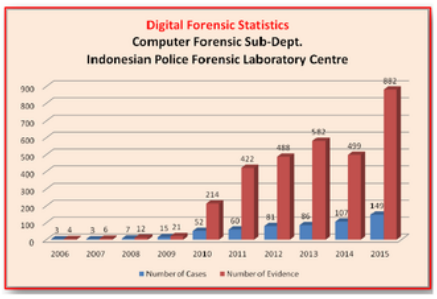


Figure 1. Computer crime statistics in Indonesia.

In criminal cases involving personal computers with the Windows Operating System, it will be a problem for investigators to find a history, file documents, as well as changes made by the offender when computer evidence is frozen hard drive. According to Faronics, DeepFreeze reducing IT support tickets by 63%, so the majority of offices and internet cafe adopt this software. In Indonesia, most of the cybercriminals prefer to access the internet in those places because their trace in browser history will be erased from memory automatically after the computer itself being restarted.

This study is expected to find digital evidence contained on the frozen hard drive by using static forensics methods. In this study, computers are as evidence that has been installed Windows XP operating system, software Deepfreeze version 5, by using the FAT32 file system.

II. BASIC THEORY

A. *Computer Forensics*

Computer forensics is related to examination and analysis of electronic evidence form of a personal computer, notebook, netbook, and tablet. Examination of evidence is usually associated with file recovery, which is a method for taking a logical file or recover deleted file or lost because there is no longer listed on the file system. The data is required to prove the crime occurred and connected with the offense (3). A file system is a method required by the computer for storage and expenditure data by providing a mechanism for data storage based hierarchy of files and directories (4).

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

All of the FAT file systems were originally developed for the IBM PC machine architecture. Thus FAT uses little endian format for entries in the BPB, FATs and File and Directory entries. In FAT32, FAT entry is 32 bits wide but only lower 28 bits are used to address 2^28 clusters. FAT32 volume can be as large as ((2^28) * 64)/2 KB which equals to 8 TB (5). From the statistics collected from W3Schools log-files, A popular operating system used is Microsoft Windows. (6).

B. *Digital Forensics Evidence*

Digital forensics is a method that relates to the recovery process and the investigation material found on digital evidence, as part of the investigation (7). Digital evidence is fragile, volatile and vulnerable if it is not handled properly. All kinds of changes containing digital evidence will lead to the wrong conclusions, or the evidence would be useless. Determination of the steps the acquisition of digital evidence performed in observance of:

- Digital media as evidence.
- The physical layout of digital storage media.
- Integrity and authenticity of digital evidence using Write-Protect, hashes, and more.
- Access to digital evidence only given for the who were given the authority and no-one the use of devices electromagnetic close to digital evidence.
- Documentation of conditions and media configuration a digital storage.
- The digital evidence duplicate/imaging using procedure and devices substandard data digital forensic acquisition.
- Documentation of information and do the configuration on digital devices.
- The statements above are based on Regulation of General Inspector for Indonesia Ministry of Finance on guidelines for digital forensic examination on the general inspectorate [8].

C. *Static Forensics Analysis*

The static forensics analysis referred to the traditional forensic investigation that is executed on such data which is at rest, for instance, the different contents of a hard drive when the computer is off, it was because the data may change when the computer is on. Static forensic focused on examining the duplicate copy of the disk to retrieve the data contained within them, such as deleted files, web browsing history, network connections, user login history, and so forth. Forensic data is acquired by using different kinds of external devices like USBs, external hard drives and then this data is brought into the forensic lab for investigators to perform different kinds of operations/steps to forensically analyze evidentiary data. (9).

D. *Frozen Hard Drive*

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down the window on the left of the MS Word Formatting toolbar.

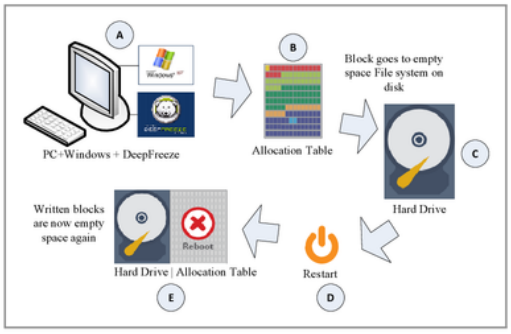


Figure 2. Deep freeze workflow

In figure 2, point B&C shows that Deep Freeze will be stored and allocated in an empty sector on the hard drive. Then, after the computer restarts, the document files and changes that have been made will be lost.

E. *File Recovery*

File Recovery is the process of salvaging inaccessible data from corrupted or damaged when the data cannot be accessed in a normal way. Data returned from the hard drive, flash, and other storage media such as digital cameras, and camcorders. There are two techniques used for repairing data. The first one is checking for consistency and the second technique is the data carving. File recovery divided based on the types of data to find and appointed file type is shown in figure 3 (11).

Figure 3. Kind of recovery based on file type

File recovery procedure is also used in multi-cloud architectural [12]. In this study, the type of recovery used is lost file recovery which means that kind of recovery to restore files that are no longer listed in a file system under a storage media partition, but such file still in clusters and storage sectors.

III. METHODOLOGY

A. *Scenario Planning*

A scenario which has done in research is doing operations against evidence in the form of computer (PC) using an

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

operating system that Windows XP and installed Deep Freeze active, which will then called a computer test. Table 1 shown the list of scenarios performed on the computer test activities.

TABLE I. SCENARIO OF ACTIVITY

Step	Activities
1st	Copy file documents and images to desktop directory: • File .doc (MD5: 968a3fd7b0f3e650b6ae32d44f43c455) • File .xls (MD5: 4860aae2ba3a4be580e19eb28a07b8c5) • File .jpg (MD5: 6c377627f2d7f656c53be8807134baf6) • File.png (MD5 : 00ed08d4539116710fc460fefd82677c). (to get any kind of file types)
2nd	Internet browser using Firefox: • uii.ac.id • https://fit.uii.ac.id • ymail.com • yahoo search: "how to hack" (wikihow.com) (to get log internet history activity)
3th	Open the files on the flash drive: • File .txt • File .jpg (activities to obtain open recent log)
4th	Shutdown the computer.

After the operation of computer test and doing activities as on a table above, then make the acquisition.

B. *Static Acquisition*

Stages of static acquisition in this study as presented in figure 4:

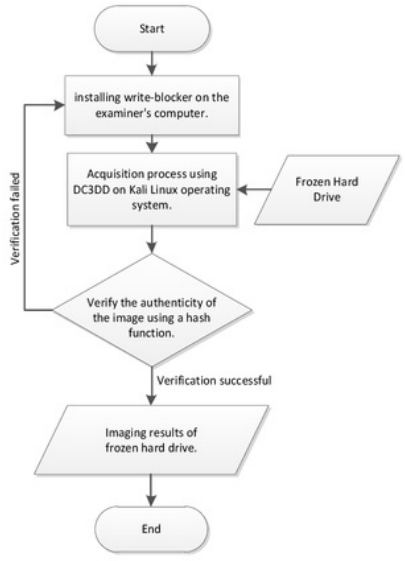


Figure 4. Static acquisition workflow

Computers tester was a computer that used in the process of acquiring.

C. *Static Analysis*

In this section, an analysis of image the results of the acquisition to find digital evidence. Digital evidence which is expected to found were document files (.doc, .xls), image files (.jpg, .png), logs the internet history , and log open recent. Flowchart of analysis will be presented in figure 5:

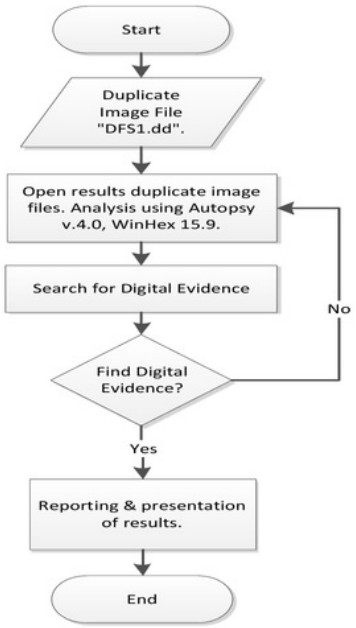


Figure 5. Forensic analysis workflow

Analysis process using autopsy software, extraction process only performed for the unallocated space.

IV. IMPLEMENTATION & RESULT

A. *Implementation of testing activity*

The process of the implementation the scenario on a computer test, are shown in figure 6:

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

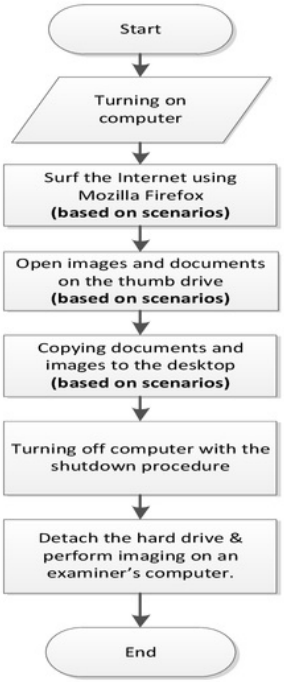


Figure 6. Scenario process implementation

Application of scenarios thought about computers tests done on that had been determined in the design scenario. With the aim to get digital evidence as on designing scenario.

B. *Acquisition Process*

In this study, the imaging process using a DC3DD tool in the Kali Linux operating system. Results from imaging to create a file named DFS1.dd, then create the value md5 hash algorithm, the results are shown in figure 7:

Figure 7. Imaging process with DC3DD

The first red box is a command to perform imaging, and the second red box is the result of the imaging process using a tool DC3DD.

C. *Analysis Process*

This section describes the steps to find digital evidence on frozen hard drives based on the scenario design. The process of analysis in this study is using two software namely Autopsy version 4.0, and version 15.9 WinHex.

The process of analysis using autopsy software only does extraction unallocated space. It is assumed that the file or logs sought are in unallocated space shown in figure 8:

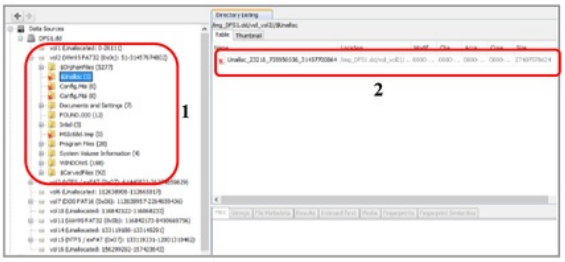


Figure 8. Autopsy extraction process.

On a red first is the list of a directory on the partition. On a red second are the contents of a directory $unalloc, which will be extracted. After the extraction then analysis using software WinHex shown in figure 9:

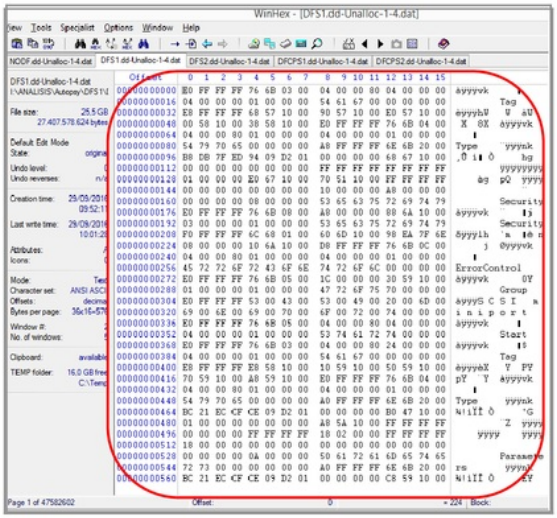
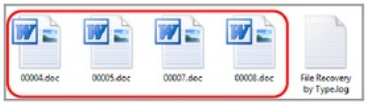
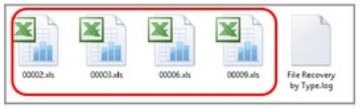
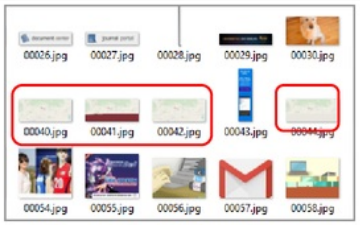
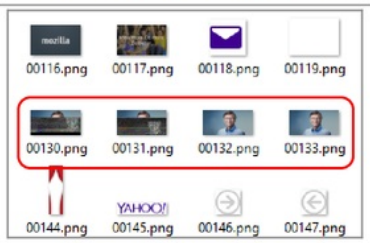
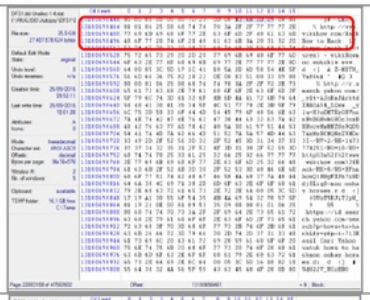


Figure 9. Extraction unallocated space on WinHex

The red box shows the contents of a file the extraction unallocated space. By using the technique carving by type, search by text string, and search by hex value and then found digital evidence sought in accordance in the draft scenarios. File with the extension .doc, .xls .jpg, and .png, was discovered using carving technique that search by file type and found that had been determined in the design scenario, so declared successful. Internet history logs found by searching techniques is the search by the hex value. Internet history logs found in accordance in the draft scenarios, so it declared a success. The open recent log is found by using searching techniques, i.e. search by text string. Open recent log found in accordance in the draft scenarios, so it declared a success. Exposure the results of digital evidence, found on table 2:

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE II. SUMMARY OF DIGITAL EVIDENCE ON THE FROZEN HARD DRIVE.

Digital Evidence	Result	Location	Information
Office file (.doc), in the red box.		Unallocated Space	Office files (.doc) is found by using a carving search by file type tool, use the keyword ".doc". MD5= 968a3fd7b0f3e650b6ae32d44f43c455
Office file (.xls), in the red box.		Unallocated Space	Office file (.xls) is found by using a carving search by file type tool, use the keyword ".xls". MD5= 4860aae2ba3a4be580e19eb28a07b8c5
Image file (.jpg), in the red box.		Unallocated Space	Image file (.jpg) is found by using a carving search by file type tool, use the keyword ".jpg". MD5= 6c377627f2d7f656c53be8807134baf6
Image file (.png), in the red box.		Unallocated Space	Image file (.png) is found by using a carving search by file type tool, use the keyword ".png". MD5= 00ed08d4539116710fc460fefd82677c
Internet history logs, in the red box.		Unallocated Space	Internet history log is found with a search by hex value tool, using the keyword: "(436B2D09)". The keyword is assumed as log header internet history on firefox.
Open recent log, in the red box.		Unallocated Space	Open recent log is found with a search by text string tool with a keyword: "(Administrator@file://)". The keyword assumed as a log file opened by user administrators.

Summary of digital evidence in this study by using software WinHex, search logs found in a manual way, while to search by file extension is found in an automated way. Document files and image files were found to have a hash value corresponding to the original file. Browsing history log using firefox and the

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

open recent log is found, matched with activity scenarios.e on the frozen hard drive.

V. CONCLUSION

In this paper, we have mentioned that Forensic engineering static acquisition which can work to the frozen hard drive on computers that have been powered off. Investigations are performed on static data of digital document files, acquired images, internet history logs, and logs the open recent in frozen hard drive found in unallocated space. All software did found on frozen hard drive refer to the following scenario to suspect is managed, as shown Table III here:

TABLE III. SYSTEM INFORMATION TOOL SOFTWARE

	Document Files		Image Files		Log Files	
	.doc	.xls	.jpg	.png	Internet History	Open Recent
Autopsy v4.0						
Winhex v15.9	√	√	√	√	√	√
Photorec v6.14						
Foremost v1.5.7			√	√		

Based on Table III, we knew that Winhex software can analysis of digital evidence more than Autopsy, Photorec, and Foremost. Analysis digital evidence from winhex software have some data such as document file found by Tools > Disk Tools > File Recovery by Type (in example: doc, xls), images found by Tools > Disk Tools > File Recovery by Type (in example : jpg, png), log internet history found by Search > Find Hex Value (using keyword "436B2D09", it assumed as header of logs internet history in firefox) log open recent found by Search > Find Text (using keyword "Administrator@file://", it also as log opened by administrator)

Installed hard drive by software deep freeze with active status, store files, logs, and something changes for the last session only. The changes are stored in unallocated space on the frozen.

REFERENCES

[1] A. Syafa'at, "Installation of Computer Forensics Using Open Source Applications". Ministry of Communications and Information Technology, 2007.

[2] M. N. Al-Azhar, "Cyber Forensic Investigation". Criminal Investigation Board Forensic Laboratory Centre, 2016.

[3] M. N. Al-Azhar, "Digital Forensic: A Practical Guide Computer Investigation". Salemba Infotek, 2012.

[4] P. Nabity, & B. J. Landry, "Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator", SWDSI, 2013.

[5] W. Ahmad, & S.M.K. Quadri, "Review of FAT data structure of FAT32 file system", Oriental Journal of Computer Science & Technology, Vol. 3(1), 161-164, 2010.

[6] W3schools, "OS Platform Statistics", w3schools, 2016. [Online]. Available: http://www.w3schools.com/browsers/browsers_os.asp. [Accessed: August-2016].

[7] V.O. Waziri, Okongwu N.O., A. Isah, O.S. Adebayo, S.M. Abdulhamid "Cyber Crimes Analysis Based-On Open Source Digital Forensics Tools", International Journal of Computer Science and Information Security, Vol. 11, pp. 30-43, Jan 2013.

[8] Ministry of Finance, "Guidelines for digital forensic examination inspectorate generals", Regulation of the inspector general of the ministry of finance, 2013.

[9] M. Rafique, & M. Khan,"Exploring Static and Live Digital Forensics: Methods, Practices and Tools". International Journal of Scientific & Engineering Research, 2013.

[10] D. C.Shettler, "Forensic Analysis of a Misused System", GCFA Practical Assigment V2.0, SANS Institute, 2005.

[11] Jasmadi, "Overcoming the lost data from virus attacks". Elex Media Komputindo, 2009.

[12] C. Pauliesther, J. Visumathi, "Towards Secure Cloud Computing Using Digital Signature", Journal of Theoretical and Applied Information Technology, 185-190, 2015.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Forensic Analysis of Frozen Hard Drive Using Static Forensics Method

ORIGINALITY REPORT

0%

SIMILARITY INDEX

PRIMARY SOURCES

1	osdev.quadlinq.com Internet	15 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		